Virtual Programmable Packet Engine (vPPE)

Enabling actionable network analytics for cloud and virtual environments

APPLICATIONS

- Real-time, network monitoring and visibility for virtual and cloud environments
- Protocol decoding and parsing for network layers 2 – 7
- Convert unstructured network data into high-resolution metadata formatted to open-standard key value pairs

BENEFITS

- Programmable, in-memory, processing technology
- Supports RegEx and entropy transcoders
- Inter-operable, easily deployed and manageable via existing analytic toolsets via a rich set of RESTful APIs

PRODUCT OVERVIEW

The virtual Programmable Packet Engine (vPPE), for container-based use cases, builds on our in-memory, stream processing capabilities of our sensor technology for physical environments and advances the evolution of network monitoring. The vPPE provides the ability to programmatically search for, extract, and deliver detailed metadata in real-time, providing an unmatched level of situational awareness, traffic visibility, and control.

The vPPE supports the deployment of network sensors in the virtual environment that DevOps and SecOps teams need to understand the characteristics and behavior of data to make decisions in real time.

PRODUCT DESCRIPTION

The MantisNet virtual Programmable Packet Engine (vPPE) sensor technology helps organizations keep pace with accelerating analytical demands and delivers data for important Time-To-Value (TTV) decisions.

IN-MEMORY COMPUTE ENGINE

Provides programmable metadata publishing engine for streaming analytic workflows

The MantisNet vPPE sensor is an in-memory, programmable decoder and metadata publishing engine that is the foundation for enabling streaming analytic workflows; providing the ability to programmatically search for, and extract detailed information about network traffic patterns, payloads, protocols and behaviors and deliver information in the form of highly efficient serialized metadata at wire-speed to data analytics platforms. It is THE wire-speed data source for network situational awareness, visibility and control. Turn your network into a data science problem!

CLOUD-READY CONTAINERS

Enables real-time monitoring of cloud/virtualized environment traffic

The vPPE provides cloud-based, or virtualized environments a containerized service that ingests native traffic and generates serialized metadata into streaming analytic pipelines. The vPPE platform is designed with the key enabling idea/abstraction that network traffic and underlying protocol contents can be represented, in data stream processing terms, as canonical tuples; key:value pairs (metadata).

HIGH-RESOLUTION NETWORK INSIGHT

THE data source for network situational awareness, visibility, and control

The vPPE generates high-resolution detail of protocols, traffic types and payloads and is designed to be used with time tested, descriptive and predictive analytic workflows. The resulting serialized metadata can be used with existing data science tools or as a source to enhance, transform, and augment data streams or batch processing, facilitating deep analytics, wire-speed traffic shaping and effecting network behavioral changes.

ENABLING CONTINUOUS MONITORING AND REMEDIATION

Understanding and acting on network behavior in real-time, in physical and virtual environments, is a challenge many organizations face. The move towards continuous monitoring and remediation can only be fully realized with wire-speed, actionable, insight - right now- of your network traffic. Historically, monitoring tools have used data-at-rest (system generated logs) to perform analytics against network traffic. This log-based approach introduces a variety of system level challenges associated with latency, and persistence of data. MantisNet's vPPE takes the next step in event-driven, wire-speed transcoding of unstructured network data into actionable intelligence allowing you to better protect your information and network assets in real-time.

THE vPPE:

- Provides real-time monitoring in the network when and where it is needed with intelligence to decode and parse any protocol and interrogate any payload type
- Utilizes protocol decoders to monitor, filter and generate specific metadata, that can be inserted anywhere in the cloud or physical networks
- Handles all network underlays, overlays and encapsulations
- Scales from lower bandwidth at individual nodes to enterprise-wide, cloud infrastructure and hybrid architectures
- Leverages containerization and orchestration tools (Docker, Kubernetes etc.) for rapid and flexible deployment
- Publishes streaming metadata, using well-known serializations, and leveraging existing data science tools
- Is simple to use, easily deployed, inter-operable with existing analytic toolsets and can be dynamically provisioned and configured

FUNCTIONALITY

- Inputs
- The vPPE supports a broad variety of common protocol decoders: some examples are GTP, DNS, DHCP, HTTP, TLS. Optionally, payload entropy, time series, and regex. decoders can convert packet traffic into protocol-specific metadata for continuous stream publishing
- Protocols are fully decoded, supporting programmatic parsing of any/all fields for extraction and follow-on processing
- Supports all manner of network underlays, overlays and encapsulations out-of-the-box
- Supports dynamic field reconfiguration; the packet parser can be updated to reverse engineer unknown, previously non-parseable headers/protocols allowing for changes as to how network packets are parsed and processed at runtime

OUTPUTS

- Converts packet traffic into serialized streams (json, avro, msgpack)
- Schema driven; extracted metadata fields are configurable and can be programmed at runtime
- Supports native ingest into a wide variety of streaming analytic frameworks and easily interfaces with a wide variety of in-memory systems; both open source platforms such as NoSQL (MongoDB, Neo4J, RethinkDB, Elastic), SQL (PrestoDB, VoltDB, PipelineDB), Heron, and Flink, as well as to commercial analytics platforms such as Splunk, SAS (ESP), Software AG (APAMA) and SAP (HANA) and TIBCO
- Interfaces with a broad range of stream processing architectures/ pipelines and management applications such as kafka, websocket, http, mqtt, s3

MANAGEMENT

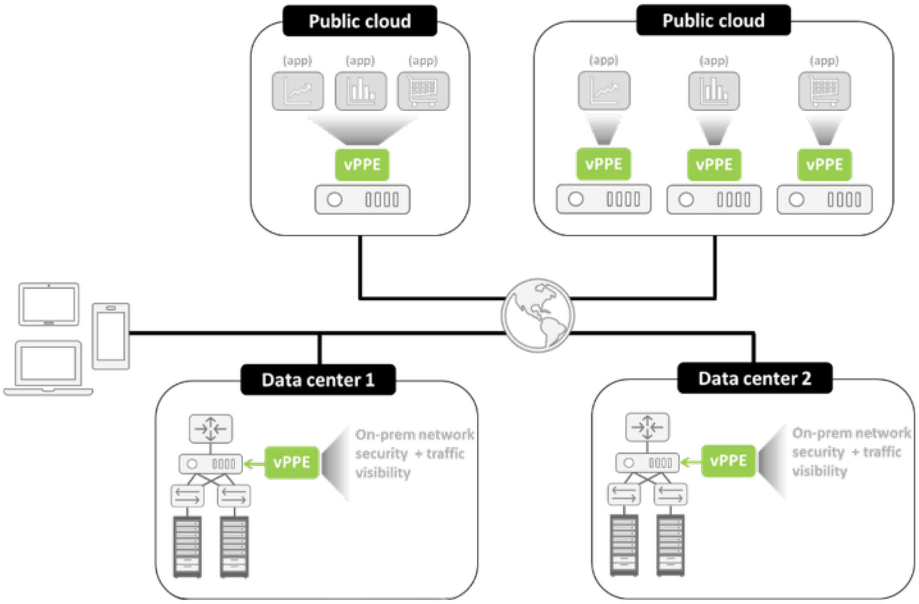
Employ's a dynamic and open management architecture

SECURITY

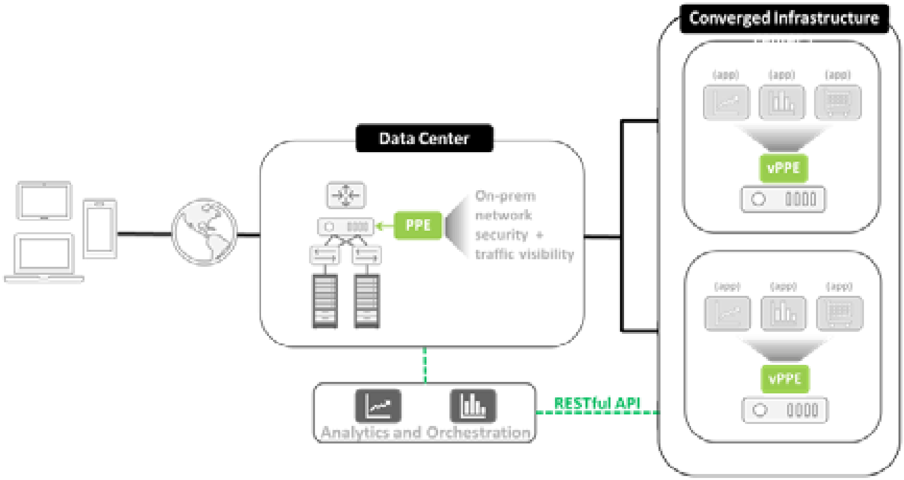
Designed with security and compliance in mind: Compliance (HIPAA, PCI-DSS, FISMA, DFARS, GDPR, ISO 27001:2013 and GPG-13) is a non-issue as event messages are optionally, cryptographically hashed to retain data lineage and there is no data persistence or archival functions: PII/PHI data is never at rest.

DEPLOYMENT OPTIONS

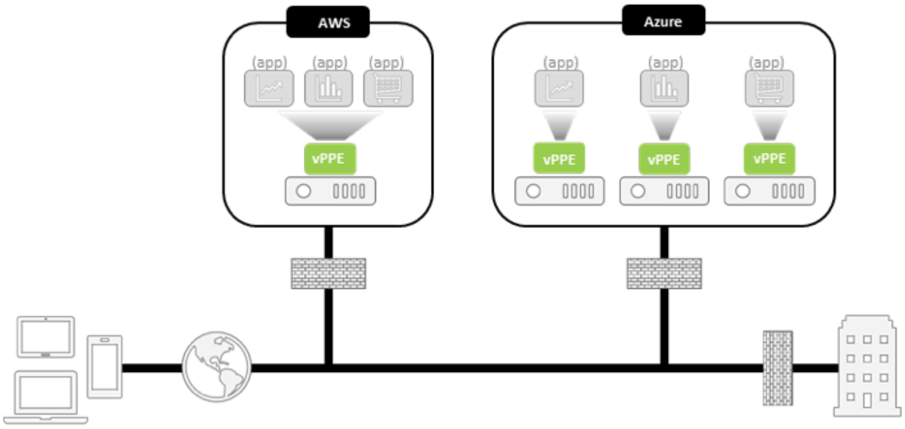
HYBRID CLOUD DEPLOYMENT ▶



PRIVATE CLOUD DEPLOYMENT ▶



PUBLIC CLOUD DEPLOYMENT ▶



SPECIFICATIONS

Available in a range of performance options; the vPPE can be sized and configured to suit the demands of the specific protocol decoders and required throughput. Maximum performance is based on throughput and capacity of available resources (network bandwidth, number of CPU cores/memory) allocated as well as the resource demands, of the specific licensed protocol decoders.

SIMPLIFIED LICENSING

- MantisNet licensing can scale with your network monitoring and protocol decoder use.
- Select PPE or vPPE and then number of decoders.
- MantisNet software licensing provide predictable lifecycle upgrades by offering support for up to two major software releases*
- Try the vPPE with a free evaluation license

ABOUT MANTISNET

MantisNet develops Software Defined Network (SDN) and Network Function Virtualization (NFV) network intelligence solutions that provide businesses and governments real-time network monitoring solutions, for 100G speeds and beyond. MantisNet's solutions better enable network teams to monitor, manage and engineer the increase in network traffic flows they're experiencing compared to the preceding generation of packet brokers, firewalls, load balancers and event management solutions.

MantisNet combines end-to-end visibility, wire-speed network monitoring and protocol analysis (from L2 to L7) with the ability to perform real-time traffic engineering and remediation against operational issues, security threats, fraud, and malicious activities, either manually or autonomously. Our solutions are deployed at leading telecom, service providers, NEM labs and government sites. We work to make network intelligence actionable for a broad range of DevOps, network and application performance testing, streaming analytics, and cyber security applications.

For more information, visit www.MantisNet.com

MantisNet
11160 C1 SOUTH LAKES DRIVE,
SUITE 190
RESTON, VA 20191
571.306.1234
INFO@MANTISNET.COM